MATHEMATICS OF COMPUTATION
VOLUME 56, NUMBER 194
APRIL 1991, PAGES 867–870

A NEW MERSENNE PRIME

W. N. COLQUITT AND L. WELSH, JR.

ABSTRACT. The number $2^{110503}-1$ is a Mersenne prime. There are exactly two Mersenne exponents between 100000 and 139268, and there are no Mersenne exponents between 216092 and 353620. Thus, the number $2^{132049}-1$ has been verified as the 30th Mersenne prime in order of size.

The Mersenne numbers $M_p = 2^p - 1$ have been studied since antiquity. One reason for their importance is that $(2^{p-1})M_p$ is a perfect number whenever M_p is prime. Earlier research resulted in the discovery of all prime M_p with $p < 100000$ [8, 10]. In addition to these 28 primes, Slowinski found that M_{132049} and M_{216091} are prime.

With the aid of the NEC SX-2 computer at HARC a systematic search for Mersenne primes M_p with p in the intervals $100000 < p < 139268$ and $216090 < p < 353620$ resulted in the 31st discovery of a Mersenne prime. This new Mersenne prime, M_{110503}, is the 29th in order of size. It is not known whether a Mersenne prime exists in the interval $139268 < p < 216090$. Every previously known Mersenne prime was verified during this search procedure, which also showed that M_{132049} is the 30th Mersenne prime in order of size. The use of the NEC SX-2 for the Mersenne prime number search was justified as a hardware verification.

The initial step in the search procedure involved trial division. Trial division is used to reduce the computational effort associated with the Lucas-Lehmer test. Prime divisors of $2^p - 1$ must have the form $2kp+1$ (where $k = 1, 2, 3, \ldots$) and simultaneously one of the forms $8n \pm 1$ ($n = 1, 2, 3, \ldots$). With the help of these facts, all potential M_p were trial factored, where $100000 < p < 524288$ with $2kp + 1$ as shown in Table 1. Steve McGrogan [6] supplied the factors $2kp + 1 < 2^{48}$ for $100000 < p < 103000$. Guy Haworth has provided us with a complete copy of his data base of residues (see below) and factors for $1 < p < 100000$ [2]. This preliminary step of trial factoring established the compositeness of 57.8% of the potential M_p.

Received January 2, 1990; revised April 9, 1990, May 22, 1990, June 19, 1990.
1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 11A41.

For all potential M_p which cannot be factored using the preliminary factor process described above, the primality is determined using the Lucas-Lehmer test [5]. The Lucas-Lehmer test states that M_p is prime if and only if M_p divides u_{p-2}, where $u_0 = 4$ and $u_i = u_{i-1}^2 - 2$ for $i \geq 1$. The remainder when u_{p-2} is divided by M_p is called the Lucas-Lehmer residue for p. The residue is zero if and only if M_p is prime.

A Fast Fourier Transform (FFT) was used to accelerate the squaring operation, which is the most time-consuming step of the Lucas-Lehmer test [3]. The standard FFT described in [9, Chapter 12] was adapted for supercomputer implementation. Adapting the 1-dimensional FFT was necessary since efficient vectorization requires a memory stride for 64-bit double-precision floating-point variables no greater than 2, and requires vectors to be as long as possible. Trigonometric array values were precomputed in quadruple precision to guarantee double-precision accuracy. Loops were split to isolate strides greater than 2, thus allowing remaining loops to reach full memory bandwidth. The real and imaginary components of the transformed data were stored in separate linear arrays to reduce memory stride. The use of the FFT speeds up the asymptotic time for the Lucas-Lehmer test for M_p from $O(p^3)$ to $O(p^2 \log p \log\log p)$ bit operations. An FFT containing 8192 complex elements, which was the minimum size required to test M_{110503}, ran approximately 11 minutes on the SX-2.

The discovery of M_{110503} (January 29, 1988) has been confirmed [1, 6, 7, 11, 12]. However, some legitimate skepticism must be attached to the claim that there are no Mersenne primes in the range $216092 < p < 353620$. This is because any error in the hardware or software would almost certainly produce an erroneous residue and lead to the conclusion that M_p is composite. To address such skepticism, each step of the Lucas-Lehmer test was verified by a process similar to "casting out nines". The base used for verification was 2^{16}, since 16 bits were used in each floating-point array element. For $p > 278528$ the array used by the FFT had 2^{15} elements, each containing 16 bits, hence the radix 2^{16} digits were summed modulo $2^{16} - 1$. For $p < 278528$ the array used by the FFT had 2^{14} elements, each containing 17 bits, and checksum arithmetic was done with modulo $2^{17} - 1$. The correctness of each squaring operation was checked by verifying that the square of the sum of the digits was congruent to the sum of the digits of the square modulo $2^{16} - 1$ (or $2^{17} - 1$). The probability that an error would go undetected is only about 2^{-16}. Over a three-year period, this comparison has resulted in one hardware error per annum. In addition, both software and hardware have been tested by favorable comparison of our results with the reported low-order 15 bit Lucas-Lehmer residues for $p < 100000$ [2, 4, 6]. Some of the low-order 15 bit residues are given in Table 2. This extensive testing and comparison of results implies that the probability of error is quite small, but nonzero.

TABLE 1
Factoring depth

Range of p	$2kp + 1$
$100000 < p < 103500$	48 bits
$103500 < p < 229836$	47 bits
$229836 < p < 270000$	41–48 bits
$270000 < p < 300000$	47 bits
$300000 < p < 355036$	44–50 bits
$355036 < p < 521244$	44 bits
$521244 < p < 524288$	47–50 bits

TABLE 2
Example residues

(The full 1Mb ASCII database is available from c46walt@harc.edu.)

p (decimal)	Residue (octal)
43067	21556
139199	75436
179717	51223
200231	11161
255709	15275
312581	06462
384301	34001
421493	23673
459649	21173
524269	70207

ACKNOWLEDGMENTS

The authors thank the Houston Area Research Center for donation of computer time. We are also grateful to the anonymous referee whose suggestions made this paper far better than it would have been otherwise.

BIBLIOGRAPHY

1. D. H. Bailey, personal communication.
2. G. Haworth, personal communication (graciously supplied both information and verification data for $p < 100000$).
3. D. Knuth, *The art of computer programming*, Vol. 2, 2nd ed., Addison-Wesley, 1981, pp. 290–295.
4. S. Kravitz and M. Berg, *Lucas' test for Mersenne numbers*, $6000 < p < 7000$, Math. Comp. **18** (1964), 148–149.

5. D. H. Lehmer, *On Lucas's test for the primality of Mersenne's numbers*, J. London Math. Soc. **10** (1935), 162–165.

6. S. McGrogan, personal communication.

7. H. Nelson, personal communication.

8. C. Noll and L. Nickel, *The 25th and 26th Mersenne primes*, Math. Comp. **35** (1980), 1387–1390.

9. W. H. Press, B. P. Flannery, S. A. Teukolsky, and W. T. Vetterling, *Numerical recipes*, Cambridge Univ. Press, 1986, pp. 386–395.

10. D. Slowinski, *Searching for the 27th Mersenne prime*, J. Recreational Math. **11** (1978–79), 258–261.

11. ____, personal communication.

12. J. Young, personal communication.

HOUSTON AREA RESEARCH CENTER, 4802 RESEARCH FOREST DR., THE WOODLANDS, TEXAS 77381